TÜVRheinland®
Precisely Right.

Automation, Functional Safety

Test report of the type approval of GuardLogix- SIL3-Controller L7xS/ L7SP of Rockwell Automation

Report-No.: 968/M 338.00/12
Date: 2012-02-08

Test report of the type approval of
GuardLogix- SIL3-Controller L7xS/ L7SP
of Rockwell Automation

Report-No.:	968/M 338.00/12
Date:	2012-02-08
Pages:	28
Test object:	GuardLogix- SIL3-Controller - 1756-L7xS primary controller - 1756-L7SP safety partner
Customer /Manufacturer:	Rockwell Automation Inc. Safety Logix Systems 1201 South Second Street Milwaukee, WI 53204 United States of America
Order-No./Date:	PO 5500003122 dated 2011-07-20
Test Institute:	TÜV Rheinland Industrie Service GmbH Automation, Functional Safety Am Grauen Stein 51105 Köln Germany
TÜV-Offer-No./Date:	968/211/11 dated 2011-05-02
TÜV-Order-No./Date:	1066 5167 dated 2011-06-24
Inspector:	Dipl.-Ing. Robert Heinen Dipl.-Ing. Gernot Klaes
Test location:	see Test Institute
Test duration:	October 2010 - February 2012

The test results are exclusively related to the test samples.

This report must not be copied **in an abridged version** without the written permission of the Test Institute.

Contents **Page**

1.	Scope	5
2.	Standards forming the basis for the requirements	5
3.	Identification of the test object	6
3.1.	Description of the device under test	6
3.2.	Documents	7
3.3.	Test object	9
3.4.	Previous test reports	10
4.	Tests and test results	10
4.1.	General	10
4.2.	Definition of the safety requirements	11
4.3.	Description and result of the inspection of the safety structure	11
4.4.	Requirements in accordance with IEC 61508	11
4.4.1.	Assessment of the management of functional safety	12
4.4.2.	Documentation over the entire life cycle	12
4.4.3.	Assessment of the measures for controlling failures in hardware	12
4.4.4.	Assessment of the measures for failure avoidance in hardware/software	13
4.4.5.	Safety related parameter PFD, PFH and SFF	13
4.4.5.1.	Safety related parameter SFF	13
4.4.5.2.	Safety related parameter PFD and PFH	13
4.4.6.	ICE1 ASIC	14
4.5.	Embedded software / firmware changes	14
4.6.	Function blocks / safety application instructions DCA and DCAF	15
4.7.	Fault insertion tests, functional test and main approval	15
4.8.	Electrical safety	16
4.9.	Environmental tests	16
4.9.1.	Temperature, climate, vibration and shock	16
4.9.2.	EMC	16
4.9.3.	Enclosure protection degree	17

Contents **Page**

4.10.	Accompanying documents	17
4.11.	Application specific considerations	17
4.11.1.	Requirements according to EN ISO 13849-1	17
4.11.2.	Requirements according to EN 60204-1	18
4.11.3.	Requirements according to EN 50156-1	18
4.11.4.	Requirements according to EN 746-1+A1, EN 746-2	18
4.11.5.	Requirements according to IEC 61511-1	19
4.11.6.	Requirements according to ANSI/RIA R15.06	19
4.11.7.	Requirements according to ANSI B11.19	21
4.11.8.	Requirements according to NFPA 79	22
4.11.9.	Requirements according to NFPA 85	24
4.11.10.	Requirements according to NFPA 86	26
4.12.	Programming and configuration	28
4.13.	Communication requirements	28
5.	Summary	28

1. Scope

The GuardLogix Controller series 1756-L7xS and its safety partner 1756-L7SP (in the following just named as Safety Controllers) has been type approved against the requirements of EN ISO 13849-1:2008, PL e and IEC61508 / EN 62061, SIL 3.

Only those components were in the scope of this type approval, which are listed in chapter 3.4. All modules, which are listed in the "GuardLogix PLC Revision Release List Rockwell Automation Certificate No.: 01/205/5088/10", were not in the scope of this approval.

Based on this type approval an EC-Type examination certificate shall be issued.

2. Standards forming the basis for the requirements

[S1] IEC 61508, parts 1 - 7: 2010
Functional safety of electrical/electronic/programmable electronic safety-related systems

[S2] EN ISO 13849-1:2008 + AC:2009
Safety of machinery - Safety-related parts of control systems -
Part 1: General principles for design

[S3] EN 62061:2005 + corrigenda 2006, 2009, 2010
Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

Application specific standards

[S4] EN 61511-1:2004 (IEC 61511-1:2003)
Functional safety - Safety instrumented systems for the process industry sector
Part 1: Framework, definitions, system, hardware and software requirements

[S5] NFPA 79:2012
Electrical Standard for Industrial Machinery

[S6] NFPA 85:2011
Boiler and Combustion Systems Hazards Code

[S7] NFPA 86:2011
Standard for Ovens and Furnaces

[S8] ANSI B11.19:2010
American National Standard for Machine Tools
- Performance Criteria for Safeguarding

[S9] ANSI/RIA R15.06:1999
American National Standard for Industrial Robots and Robot Systems
- Safety Requirements

[S10] EN 50156-1:2004
Electrical equipment for furnaces and ancillary equipment
Part 1: Requirements for application design and installation

[S11] EN 60204-1:2006
Safety of machinery - Electrical equipment of machines;
Part 1: General requirements

[S12] EN 746-1:1997+A1:2009
Industrial thermoprocessing equipment
Part 1: Common safety requirements for industrial thermoprocessing equipment;

[S13] EN 746-2:2010
Industrial thermoprocessing equipment
Part 2: Safety requirements for combustion and fuel handling systems;

Electrical safety and resistance against environmental conditions

[S14] IEC 61131-2:2007
Programmable Controllers - Equipment requirements and tests

[S15] EN 50178:1997
Electronic equipment for use in power installations

[S16] EN 61326-3-1:2008
Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications

Failure rates of components

[S17] SN29500: 2004-2009
Failure rates, components, expected values, dependability

3. Identification of the test object

3.1. Description of the device under test

The GuardLogix Controller series 1756-L7xS consist of a primary controller and a safety partner 1756-L7SP. The primary controller will handle safety and non safety related tasks, communication to (external) devices like I/O-components and communication to the safety partner. The safety partner itself will only run the safety tasks and report its results to the primary controller for comparison and completing safety messages. For a complete safety system DeviceNet and/or EtherNet/IP safety I/O-components can be used to build up safety loops. Safety related messages are exchanged using the CIP-Safety protocol.

This basic concept has been taken over from the previous GuardLogix- SIL 3-Controller project (see also [R1]). The embedded software / firmware of the previous GuardLogix-SIL 3-Controller project has been re-used and just adapted to the new hardware platform. The original GuardLogix controller was based on an ASIC, called ATLAS, which contains the microprocessor together with peripheral elements. In the new Safety Controller ATLAS was replaced by a new ASIC, called ICE1. Existing tests were re-run to verify that there are no regressions. Due to the fact that the diagnostic domain is tightly coupled to the hardware platform, several parts of the diagnostics are new or changed including the respective software. The existing CIP-safety communication protocol has been integrated into the new Safety Controllers. The programming and configuration tools have been taken over from the previous controller projects.

The ICE1 ASIC was designed from scratch only re-using several units within its design from former projects. Because of the new ASIC all the hardware parts around this ASIC have either been adjusted or have been developed from scratch.

3.2. Documents

The complete project documentation for development, design, testing and quality management are summarized and stored on the TÜV Rheinland file server.

Among others the following superior documents have been provided to the Test Institute:

No.	Superior document	Date	Revision
[D1]	SRS Validation_Verification Package Document List file: Document_List_Ver2_2_1_12.doc embedded in file: 1756_L7xS Safety Plan and VnV Plan RevD 2_1_12.docx	2012-02-01	-/-
[D2]	Safety Concept 1756-L7xS File: Safety Concept 1756-L7xS Rev 13 10_4_11.doc	2011-10-04	13
[D3]	1756-L7xS GuardLogix V20 FUNCTIONAL SAFETY MANAGEMENT DOCUMENTATION file: 1756_L7xS Safety Plan and VnV Plan RevD 2_1_12.docx	2012-02-01	D
[D4]	Functional Block-Level FMEA file: FMEA_B Logix Integrated Safety L7xS.xlsx	2011-10-04	13.0
[D5]	FMEA - L7xS SIL3 GuardLogix Integrated Safety File: FMEA Logix Safety L7xS_Ver 13 10-4-11.doc	2011-10-04	13.0
[D6]	L7xS FMEA File: FMEA L7xS_Ver 13 10_4_2011.xlsx	2011-10-04	13.0
[D7]	ICE ASIC Design Summary File: DesignSummary_Ice_v2.xlsm	2011-12-09	2
[D8]	Ice Logix Processor ASIC Verification Summary File: Ice_Verification_Summary.doc	2011-11-11	0.4
[D9]	New ASIC Process SIPOC - ICE ASIC File: New ASIC Process SIPOC v11 - ICE ASIC_v2.xlsm	2011-12-09	2
[D10]	Ice Logix Processor ASIC, Functional Safety Assessment File: Ice_ASIC_Functional_Safety_Assessment_v1.1.docx	2012-01-31	1.1
[D11]	Design Description, Embedded Software Design - Logix Integrated Safety File: Embedded Software Design - Logix Integrated Safety_DRAFT_03.doc	2011-07-19	Draft 03
[D12]	Design Description, Embedded Software Design - L7x Diagnostics File: Embedded Software Design - L7x_L7xS Diagnostics V7 12_6_11.doc	2011-12-06	7
[D13]	GuardLogix V20 Dual Channel Analog Input Instructions FRS File: GuardLogix V20 Dual Channel Analog Input Instruction.doc	2011-07-12	1.7
[D14]	Logix Code Base Impact Assessment File: LogixCodeBaseImpactAssessment.doc	2011-04-28	0
[D15]	ESW Quality Report File: ESW Quality Report L7xS GuardLogix.doc	2011-01-27	0
[D16]	Safety Related Code Checkpoint R20_01 File: CheckpointReview_R20_01.pdf	2010-11-03	-
[D17]	Safety Related Code Checkpoint R20_02 File: CheckpointReview_R20_02.pdf	2011-08-31	-
[D18]	Safety Related Code Checkpoint R20_03 File: CheckpointReview_R20_03.pdf	2011-10-12	-
[D19]	Safety Related Code Checkpoint R20_04 File: CheckpointReview_R20_04.pdf	2012-01-10	-

No.	Superior document	Date	Revision
[D20]	Safety Related Code Checkpoint R20_05 File: CheckpointReview_R20_05.pdf	2012-01-23	-
[D21]	Fault Insertion Report File: 1756-L7x Fault_Insertion Test Plan_Report 2011-12-13.pdf	2011-12-13	00.12
[D22]	Fault Insertion Report File: 1756-L7x Fault_Insertion Test Plan_Report 2011-12-13.xlsx	2011-12-13	00.12
[D23]	Certificate No. CERT-09379-2004-USA-RvA Rev. 1 File: 9001_shared_certificate_2011.pdf	2011-03-10	-
[D24]	GuardLogix Safety Protocol Conformance Test Strategy File: GuardLogix Safety Protocol Conformance 2_2.docx	2012-01-27	2.2
[D25]	Safety Protocol Test Summary File: Safety Protocol Test Summary.doc	2012-01-27	00
[D26]	Safety Controller EMC Test Report (Test Report #848238) File: 1756-L7S EMC TR.pdf	2012-01-20	-
[D27]	Safety Controller Temperature and Humidity Test Report (Test Report #557192) File: Temp Humidity Report 557192.pdf	2012-01-24	-
[D28]	Safety Controller Shock and Vibration Test Report (Test Report #30552) File: Packaged ShocknVib Report 30552.pdf	2012-01-25	-
[D29]	Safety Controller Shock and Vibration Test Report (Test Report # Test Report #609711) File: Unpackaged ShocknVib Report 609711.pdf	2012-01-24	-

Besides the above listed documents, the customer has provided the following user manuals:

No.	User manuals	Date	Revision
[U1]	Safety Reference Manual GuardLogix Controller Systems File: 1756-RM093G-EN-P.pdf	2012	G
[U2]	User Manual GuardLogix Controller Systems File: 1756-UM020G-EN-P.pdf	2012	G
[U3]	Safety Reference Manual GuardLogix Safety Application Instruction Set File: 1756-RM095E-EN-P.pdf	2011	E
[U4]	Product Information File: 1756-PC006A-EN-P.pdf	2012	A

The following table shows the main documents, compiled by the Test Institute:

No.	Document by the Test Institute	Date	Revision
[T1]	Fault-Insertion-Test on L7x, L7xS controller system File: RA_FIT_L7x-L7xS_V1_3_2011-11-29-COMPLETE.doc	2011-11-29	1.3
[T2]	Questions regarding ASIC development and use File: ICE1_TUV_2011-03-25.doc	2011-03-25	1.0
[T3]	Checklist Techniques and Measures for ASICs File: ICE1_ASIC_Checklist_ASICS_IEC61508_v1.xls	2012-01-09	1.0
[T4]	List of open points, IEC1 ASIC - Rockwell Automation File: RA_ICE1_LOP_TUV_2012-02-01.xls	2012-01-31	-
[T5]	Test Plan Rockwell L7x_ L7xS; File: TUV_EnvTestPlan RAI L7x_ L7xS_V2_Results_TUV_2012-02-01.doc	2012-02-01	-
[T6]	GuardLogix PLC Revision Release List; File: 2012-02-08	2012-02-08	1.0

3.3. Test object

The following products and their revisions are covered by this type approval:

Type designation	Component description	HW - Revision	Firmware Revision
GuardLogix Product Family			
1756-L72S	Primary Controller (Logix 5572S) with 4 MB Memory	Series B	Version 20
1756-L73S	Primary Controller (Logix 5573S) with 8 MB Memory	Series B	Version 20
1756-L7SP	Safety Partner (Logix L7SP)	Series B	Version 20
GuardLogix Extended Temperature Product Family			
1756-L73SXT	Primary Controller (Logix 5573SXT) with 8 MB Memory	Series B	Version 20
1756-L7SPXT	Safety Partner (Logix L7SPXT)	Series B	Version 20
Programming and Configuration			
RSLogix5000	Programming and configuration Tool for 1756-L7xS and 1756-L73SXT controllers	-/-	Version 20

	Type designation	Component description	HW - Revision
	1756-ESMCAP	L7x Energy Storage Module-CAP	Series B
	1756-ESMNRM	L7x Energy Storage Module Non Removable	Series B
•	1756-ESMNSE	L7x Energy Storage Module No Stored Energy	Series B
•	1756-ESMNSEXT	L7x Energy Storage Module No Stored Energy- Extended Environment	Series B
	1756-ESMCAPXT	L7x Energy Storage Module CAP-Extended Environment	Series B
	1756-ESMNRMXT	L7x Energy Storage Module Non Removable – Extended Environment	Series B
•	1756-SPESMNSE	L7SP Energy Storage Module No Stored Energy	Series B
	1756-SPESMNRM	L7SP Energy Storage Module Non Removable	Series B
•	1756-SPESMNSEXT	L7SPXT Energy Storage Module No Stored Energy – Extended Environment	Series B
	1756-SPESMNRMXT	L7SPXT Energy Storage Module Non Removable – Extended Environment	Series B

Note: In explosive environments only ESM/ESMCAP types designated as having "no stored energy" (indicated by a dot in the table) can be used, because the capacitor for the real-time clock (which may not fully discharge) is not present.

Most of the test activities were based on documents, which were provided by the manufacturer. In addition, practical tests have been performed by the Test Institute together with the design engineers during the fault insertion tests (see chapter 4.8 for details). The IDs of the used test samples are documented and can be found in the inspectors fault insertion test documentation.

3.4. Previous test reports

[R1] 968/EZ 191.00/05 dated 2005-01-31
Report of the type approval of the GuardLogix-SIL 3-Controller of Rockwell Automation

[R2] 968/EZ 191.01/05 dated 2005-11-07
Report of the approval of different changes of the GuardLogix Controller

[R3] 968/EZ 191.02/07 dated 2007-01-31
Report of the additional type approval of GuardLogix-SIL 3-Controller of Rockwell Automation

[R4] 968/EZ 191.03/07 dated 2007-04-30
Report of the additional type approval of GuardLogix-SIL 3-Controller of Rockwell Automation

[R5] 968/EZ 191.04/07 dated 2007-10-29
Report of the approval of different changes of the GuardLogix Controller of Rockwell Automation

[R6] 968/EZ 191.05/08 dated 2008-02-27
Report of the approval of different changes of the GuardLogix Controller V16.21 of Rockwell Automation

[R7] 968/EZ 191.06/08 dated 2008-09-15
Test report about the inspection of various function blocks and the additional type approval of GuardLogix-SIL 3-Controller of Rockwell Automation

[R8] 968/EZ 191.07/09 dated 2009-08-26
Report of the approval of different changes of the GuardLogix Controller V17.07.59

[R9] 968/EZ 191.08/10 dated 2010-03-04
Test report about the supplementary type approval and certification of the GuardLogix controller

[R10] 968/EZ 191.09/10 dated 2010-03-30
Test report on the supplementary type approval and certification of the GuardLogix controller

[R11] 968/EZ 191.10/10 dated 2010-10-15
Test report on the supplementary type approval and certification of the GuardLogix controller

4. Tests and test results

4.1. General

The measuring and test equipment, which has been used by the TÜV Rheinland Group in the tests described in the following, is subject to regular inspection and calibration. Only devices with valid calibration have been used. The devices used in the various tests are recorded in the inspector's documentation.

All considerations concerning uncertainty of the measurements, so far applicable, are stated in the inspector's documentation, too.

In cases where tests have been executed in an external test lab or in the test lab of the manufacturer and where the results of these tests have been used within the here documented approval, this has occurred after a positive assessment of the external test lab and the achieved test results in detail according to the Quality Management procedure QMA 3.310.05.

4.2. Definition of the safety requirements

The Safety Controllers must comply with the general requirements for fail-safe controls in accordance with:

- EN ISO 13849-1:2008 Category 4, PL e
- EN 62061:2005 SIL CL 3
- IEC 61508:2010 SIL 3

Due to the technology in the device and the intended application it is considered as a type B subsystem in accordance with [S1] part 2. It operates beside as a component for a protective device in a "Low Demand Mode of Operation" also in "High Demand Mode of Operation" applications.

4.3. Description and result of the inspection of the safety structure

The Safety Controllers are designed as a dual channel solution (HFT = 1), consisting of a primary controller and its partner, with mutual monitoring and comparison as well as continuously running diagnostics functions in each channel. The implemented diagnostic functions have at least a diagnostic coverage of DC = 90 % (medium). Furthermore, each channel has its own logic power-supply.

The communication between the primary and safety partner is temporally and logically monitored.

In the case of an internal failure condition the Safety Controllers change to the lockout state, ceases bus communication and displays this state.

The inspection of the safety structure was performed essentially on documentation level. During these inspections the overall safety structure as well as in particular the hardware and software were assessed. The major basis for the inspection was the safety concept description ([D2]).

Together with the software, hardware designer, quality management engineers and project leader the measures for failure avoidance and failure control as per [S1] - [S3] were verified during the fault insertion test (see chapter 4.6). Furthermore the manufacturer has performed a FMEA on block level [D5], [D6]. The results are available at the Test Institute.

Result:

The safety structure complies with the requirements in [S2] for safety category 4.

4.4. Requirements in accordance with IEC 61508

The Safety Controllers shall meet the requirements for Safety Integrity Level 3 (SIL 3) of [S1] and [S3].

The following points have been assessed:

- management of functional safety
- documentation over the entire life cycle

- measures for controlling failures in hardware
- measures for failure avoidance in hardware/software
- safety related parameters

4.4.1. Assessment of the management of functional safety

The Functional Safety Management in the Safety Controller project (excluding the ICE1 ASIC development) is documented in the Safety-Plan and V&V-Plan (see document [D2]). The document has been reviewed. Further more the functional safety management system has been audited by the Test Institute on project level in spot checks (see document [T1]) The Functional Safety Management of the ICE1 ASIC development has been assessed separately in chapter 4.4.6.

Result:

The Safety-Plan and V&V-Plan fulfill the requirements of [S1]. The spot checks did not show any indication that respective requirements are not met.

4.4.2. Documentation over the entire life cycle

The Safety-Plan and V&V-Plan (see document [D3]) includes the planned documentation over the entire life cycle. The documents have been reviewed by the Test Institute. Open items have been discussed and clarified together with the customer [T4]. The documentation of the ICE1 ASIC development is listed separately. Chapter 4.4.6 gives further information.

Result:

The assessment of the documentation on the Safety Controller confirmed that the respective requirements of [S1] are met.

4.4.3. Assessment of the measures for controlling failures in hardware

The Safety Controllers have been assessed for conformance to the safety integrity requirements acc. to SIL 3 of [S1] and acc. to safety category 4 of [S2].

The implemented hardware and software measures for failure detection have been analyzed by the manufacturer and verified by the Test Institute, if they are suitable and sufficient to detect the failures, which have to be assumed acc. to table A.1 in [S1] part 2, and if the combination of 2 faults cannot result in a fail to danger acc. to [S2], if the first fault remains undetected.

The manufacturer has performed Failure Mode and Effects Analyses (FMEA) on system and on block level, in order to show, that the SIL 3 and safety category 4 requirements are complied with. The documents [D4], [D5], [D6] with the results of these analyses are available at the Test Institute.

Any detected fault will result in the configured fault reaction, which by default is the deactivation of the CIP-Safety communication to I/O-components.

The properties of the Safety Controllers and the requirements of the specification were checked; both with positive tests (functional verification) as well as with negative tests (fault insertion). These tests were carried out in co-operation with the Test Institute at the manufacturer's premises.

Result:

It can be confirmed that the applied measures for controlling failures meet the requirements of [S1], [S2].

4.4.4. Assessment of the measures for failure avoidance in hardware/software

The assessment of fault avoidance in the hardware and software of the Safety Controller was part of the functional safety management (see chapter 4.4.1 and 4.4.2). The planned measures have been reviewed by the Test Institute. The application of the planned measures has been verified in spot checks during the main approval (see document [T1]). Open items have been clarified in discussions together with the customer. The measures for fault avoidance during the development of the ICE1 ASIC have been reviewed separately in chapter 4.4.6.

Result:

The respective requirements of [S1] are fulfilled.

4.4.5. Safety related parameter PFD, PFH and SFF

- The common cause factors β and β_D have been determined by the manufacturer according to [S1] part 6 Annex D. The evaluation of the parameters resulted into the following values, which have been used in the PFD/PFH calculations:

  $\beta = \beta_D = 1\%$

The failure rates are based on values taken from Failure rates of components

- [S17] as well as from manufacturer data (e.g. ICE1 ASIC).
- Diagnostic elements and electronic devices used in non safety related functions were not included in failure rate calculations.

4.4.5.1. Safety related parameter SFF

The Safety Controllers are built in a complete dual channel structure. The underlying FMEA is available to the Test Institute.

Requirements for dual channel structures:

SIL 3, HFT = 1, type B components, SFF $\geq$ 90 %

Result:

The SFF of the Safety Controllers is fulfilled.

4.4.5.2. Safety related parameter PFD and PFH

The PFD_{AV} and PFH calculations have been performed by the manufacturer and were verified by the Test Institute. The underlying FMEAs are available to the Test Institute [D4], [D5], [D6].

Model	Proof Test Interval (PTI)	PFD @ PTI	PFH @ PTI
L7xS / L7SP	20 years	$8{,}9 \times 10^{-5}$	$1{,}2 \times 10^{-9}\ h^{-1}$

The safety related parameter PFD and PFH can be found in the Safety Reference Manual [U1].

Result:

The PFD and PFH meet the requirements for SIL 3.

4.4.6. ICE1 ASIC

The requirements for hardware safety integrity (random hardware faults) of the ICE1 ASIC have been considered as part of the overall Safety Controller assessment. The respective results are described in the other chapters of this report.

The requirements for systematic safety integrity of the ICE1 ASIC development have been assessed using the approach of a combination of Route 2_s or Route 3_s according to [S1] section 7.4.2.2.

The Test Institute provided to the customer a checklist [T2], which has been compiled out of the respective requirements of [S1]. As a result of the questions in this checklist the customer has gathered and compiled several documents for the ICE1 ASIC, which have been reviewed by the Test Institute. Further on the customer and Test Institute filled in a checklist regarding requirements of [S1] part 2 Annex F Table F.1 ([T3]).

The main documents are the ICE1 ASIC Design Summary ([D7]) and the ICE1 Verification Summary ([D8]). Several documents have been newly written according Route 3_s including the process specification for the ICE1 ASIC development ([D9]). Miscellaneous documents have been gathered or written according to these three prior mentioned documents and are referenced within those documents or the checklist [T2]. The key documents are available within the Test Institute.

For some units within the ICE1 ASIC the Route 3_s post-qualification approach has been chosen and for other units the Route 2_s proven-in-use method. The post-qualification approach has mainly been applied for units developed by Rockwell and the proven-in-use method has been used for Intellectual-Properties (IPs) bought from other companies (soft-cores provided by suppliers).

Further on a functional safety assessment document for the ICE1 ASIC ([D10]) has been provided. This document identifies the functionality within the ICE1 ASIC which is being utilized as part of the product level safety strategy and a summary of the verification and validation that each of these blocks underwent is described. Furthermore, all blocks that are not part of the safety strategy are identified and an analysis given as to what impact, if any, those blocks can have on the safety relevant functions.

Result:

The filled in checklists [T2] and [T3] together with the referenced documents (or documents referenced within referenced documents) and the answers in the List-of-Open-Points ([T4]) showed that all requirements of [S1] part 2 regarding systematic safety integrity and particularly of Annex B and Annex F are fulfilled. The ICE1 ASIC fulfills the requirements of a Systematic Capability of 3 (SC3).

4.5. Embedded software / firmware changes

Due to the use of the new ICE1 ASIC instead of the ATLAS ASIC

1) A new compiler has been chosen (ARM RealView compiler) which had an impact on the existing embedded software / firmware.

2) The diagnostics partly also realized in the embedded software / firmware had to be updated.

Furthermore it had been decided to

a) Add Dual Channel Analog Instructions (DCA and DCAF) as two new safety application instructions used to qualify analog input data.

b) Use the Floating Point Support of the new ICE1 ASIC which also had an impact on the existing software / firmware.

Beyond that the updated embedded software / firmware had to be integrated on the new hardware platform (some further small modifications were necessary) and the integration had to be tested. The complete list of embedded software / firmware changes is part of [D15] chapter 7.1.1.

The documentation contains:

- Design Description of the Embedded Software Design ([D11])
- Design Description of the Embedded Software Diagnostics ([D12])
- Code Base Impact Assessment due to the new compiler ([D14])
- Quality report ([D15])
- Code review reports ([D16], [D17], [D18], [D19], [D20])
- Test strategies
- Test results

All embedded software / firmware changes have been tested and reviewed. All existing tests were re-run to verify that there are no regressions.

Result:

The review of the documents came to the result that they contain sufficient information to understand the reasons for the changes.

The test results are accepted by the Test Institute.

The documentation of the changes / modifications fulfils the requirements according to [S1].

4.6. Function blocks / safety application instructions DCA and DCAF

The embedded software / firmware has been extended by two instructions for monitoring two analog input channels (for integer and real values) originating from the analog input module (see also chapter 4.5). The changes are described in detail in [D13] and have been tested by the customer like all other changes. Furthermore the function blocks have been inspected by the Test Institute during the fault insertion tests of the main approval (see chapter 4.7).

Result:

All the test results showed that the implementation of the function blocks fulfills the respective requirements.

4.7. Fault insertion tests, functional test and main approval

During the verification activities of the Safety Controller the requirements of the specification were not only checked in functional tests (positive tests) but also in negative tests (fault insertion tests). Particularly the diagnostic measures have been verified with the help of fault insertion tests. Some of these tests were carried out in co-operation with the Test Institute in the manufacturer's laboratories during the main approval.

The customer performed several fault insertion test ([D21], [D22]) as part of the verification activities. Some of these tests have been repeated and witnessed by the Test Institute as part of the main approval ([T1]). Further the Test Institute requested also positive and negative tests which have been performed mostly during the main approval at the customer premises.

Result:

The documented fault insertion tests which have been performed by the customer alone confirmed the effectiveness of the realized measures to detect and to control faults. And the functional tests and fault insertion tests performed during the main approval at the customer premises as witness tests indicated that the documented results of the functional tests and fault insertion tests carried out by the customer are trustful.

4.8. Electrical safety

Scope of this assessment was the Safety Controller 1756-L7xS and its safety partner 1756-L7SP. Both of them have to be inserted into a chassis together with a power supply module, which generates SELV / PELV. The chassis and the power supply modules are already type approved and were outside of this type approval (see [R1] for details).

The Safety Controllers are supplied with 5VDC powered from the backplane. Based on this fact the electrical safety is given.

The Safety Controllers require an Energy Storage Module (ESM/ESMCAP) to supply the energy to the main board to save the state of the controller at loss of power. The electrical energy in the capacitor based ESM/ESMCAP is stored in a high voltage capacitor and need to be assessed regarding whether the electrical safety is given. The ESMCAP includes an additional capacitor for the real-time clock.

The ESM/ESMCAP is designed such that no high voltage can be touched by a person nor can feed to the controller itself. This was evaluated in theory and furthermore practically verified even under fault conditions. Under no circumstances voltage higher than SELV appears outside of the module.

Result:

The electrical safety based on [S14] and [S15] of the Safety Controllers together with the ESM/ESMCAP is given In explosive environments only ESM/ESMCAP types designated as having "no stored energy" can be used, because the capacitor for the real-time clock (which may not fully discharge) is not present.

4.9. Environmental tests

4.9.1. Temperature, climate, vibration and shock

The temperature and mechanical tests were carried out based on the requirements defined in [S14]. All tests have been performed at the Rockwell Automation EMC Test Laboratory in Mayfield Heights ([D27], [D28], [D29]). **Fehler! Verweisquelle konnte nicht gefunden werden.**This laboratory was assessed by Bureau Veritas for temperature, climate and vibration. Due to the fact that the shock test are performed on the same calibrated equipment, by the same trained individuals, under the same lab procedures and controls as the vibration test, the Test Institute judged the assessment results of Bureau Veritas also to be valid for the shock tests.

Result:

All tests have been passed and are accepted by the Test Institute.

4.9.2. EMC

The EMC and immunity tests were carried out based on the requirements defined in [S14] for normal levels and [S16] for increased immunity levels. All tests have been performed at the accredited Rockwell Automation EMC Test Laboratory in Mayfield Heights ([D26]**Fehler! Verweisquelle konnte nicht gefunden werden.**). This laboratory was accredited for Electromagnetic Capability and Telecommunications by the United States Department of Commerce National Institute of Standards and Technology.

The radiated emission was tested at the same facilities and fulfils the requirements defined in [S14].

Result:

All tests have been passed and are accepted by the Test Institute.

4.9.3. Enclosure protection degree

The Safety Controllers must be mounted within an enclosure that is suitably designed for those application specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The interior of the enclosure must be accessible only by the use of a tool (see [U1]).

Result:

The User Manual gives detailed information in order to ensure proper mounting and therefore maintaining the protection degree.

4.10. Accompanying documents

The accompanying documents [U1] - [U3] based on the former GuardLogix-SIL3-controller system and were modified according to the new Safety Controllers need. [U3] was supplemented by two new function blocks / safety application instructions (see also chapter 4.6):

- Dual-channel Analog Input (DCA) - integer version
- Dual-channel Analog Input (DCAF) - floating point version

The Safety Reference Manuals [U1], [U3] and the User Manual [U2] for the GuardLogix-SIL 3-controller system has been reviewed. They contain the necessary information for the correct installation and safe operation.

The product information [U4] was reviewed with regards to the machinery directive requirements Annex I, 1.7.4.2. It contains all necessary information.

Result:

The accompanying documentation contains the necessary information for a correct installation and safe operation.

4.11. Application specific considerations

4.11.1. Requirements according to EN ISO 13849-1

The Safety Controllers fulfill the requirements of [S1] up to SIL 3, [S2] up to category 4 and the designated architecture as per chapter 6.2.7.

[S2] chapter 4.6.2 requests that the software design and development process of a SRESW for PL = e shall comply with [S1] part 3, SIL 3. This requirement is fulfilled.

As per table 3 in [S2], in general it is possible to achieve a PL = e for complex, programmable electronics, provided that the average probability of dangerous failure per hour (PFH) of the components are less than the maximal stated value for PL = e. The PFH values of the devices are listed in the user manual.

The $MTTF_d$ value was calculated by the Test Institute based on the L7xS FMEA (for details see [D6]) by calculating the reciprocal of the sum of all dangerous failure rates λ_D. The Diagnostic Coverage was also taken over from [D6].

Model	Performance Level	Category	$MTTF_d$	Diagnostic Coverage DC
L7xS / L7SP	PL e	Cat. 4	> 100 years	medium

Result:

Since the average probability of dangerous failure per hour and the structural requirements are fulfilled, the requirements of [S2] for PL = e are also fulfilled.

4.11.2. Requirements according to EN 60204-1

The [S11] defines the general requirements for the safety of machinery, especially electrical equipment of machines. It refers mainly to the final overall application and not to special components e.g. controller.

Result:

The electrical safety as per chapter 6, the physical environment conditions as per chapter 4.4, the safety-related aspects of control functions and an appropriated level of safety performance as per chapter 9.2 and 9.4, wiring practices as per chapter 13, operating manual and maintenance manual as per chapter 17.7 and 17.8 of [S11] are fulfilled. The evidence can be found in the corresponding chapters of this report.

4.11.3. Requirements according to EN 50156-1

The [S10] lists beside the application specific requirements also system specific requirements, which are in accordance with [S1].

The technical documentation of the Safety Controllers fulfills the applicable requirements of [S10] chapter 14.

The use of the Safety Controllers inside a specific application for furnace must be evaluated separately taking into account all other requirements and boundary conditions of [S10].

Result:

The system specific requirements are fulfilled.

4.11.4. Requirements according to EN 746-1+A1, EN 746-2

These standards contain requirements for industrial thermo-processing equipment. They contain safety requirements for combustion and fuel handling systems.

In the following clauses generally relevant as well as specific requirements are defined.

Clause	Requirement	Results
EN 746-1 5.11.5	The manufacturer shall assess the effect of malfunctions of control systems/component devices in the design analysis. In the event of malfunction of a control component an unsafe situation shall not arise (see [S2]).	Fulfilled
EN 746-2 5.7.2	Requirements for protective systems b) hardwiredsystem with a combination of components complying with the relevant product standards as specified in 5.2 to 5.6 and of components complying with defined SIL/PL in accordance with [S3] and [S2] respectively; - guarding functions (e.g. gas pressure, temperature) performed by components for which no relevant product standards are existing shall comply with at least SIL 2/PL d;	L7xS can be used for monitoring as well as for safety function

Clause	Requirement	Results
EN 746-2 5.7.2 (cont.)	- functions which will lead to immediate hazard in case of failure (e.g. flame detector device, ratio monitoring) performed by components for which no relevant product standards are existing shall comply with at least SIL 3/PL e;	
EN 746-2 5.7.2	c) PLC based system with a combination of components complying with the relevant product standards as specified in 5.2 to 5.6 and of components complying with defined SIL/PL; - guarding functions (e.g. gas pressure, temperature) performed by components for which no relevant product standards are existing shall comply with at least SIL 2/PL d; - functions which will lead to immediate hazard in case of failure (e.g. flame supervision, ratio control) performed by components for which no relevant product standards are existing shall comply with at least SIL 3/PL e; - software for safety functions should be separate from other functions (e.g. control functions). The software for safety functions shall be designed in accordance with the requirements of [S2] or [S3]. - a PLC used for safety functions shall comply with [S2] or [S3];	L7xS can be used for monitoring as well as for safety function Functional requirements as specified in chapter 5.2 to 5.6 of this standard have to be observed separately.
EN 746-2 5.7.2	d) PLC based system in which all components comply with defined SIL 3/ PL e and with a defined SIL 3/ PL e of hard and software; - in this case [S2] and [S3] shall be applied for the protective system in general.	L7xS can be used for monitoring as well as for safety function Functional requirements as specified in chapter 5.2 to 5.6 of this standard have to be observed separately.

Result:

The specific requirements are fulfilled.

4.11.5. Requirements according to IEC 61511-1

The Safety Controllers fulfill the requirements for SIL 3 in accordance with [S1].

Result:

The system can be used within the scope of [S4].

4.11.6. Requirements according to ANSI/RIA R15.06

This American National Standard applies beside the manufacture, remanufacture, re-build, installation, maintenance, testing, start-up and training also to the safeguarding requirements for industrial robots and robot systems.

It defines methods of safeguarding to enhance the safety of personnel associated with the use of robots and robot systems.

In the following clauses generally relevant as well as specific requirements are defined.

Clause	Requirements	Result
4.5.3	Single channel with monitoring safety circuits shall include the requirements for single channel, shall be safety rated, and shall be checked (preferably automatically) at suitable intervals.	The Safety Controllers are partly built as single channel. Their functions are automatically tested within the function in background.
4.5.4	Control reliable safety circuitry shall be designed, constructed and applied such that any single component failure shall not prevent the stopping action of the robot.	This requirement is fulfilled. See previous chapters.
5.3	Requirements for other safeguarding devices that signal a stop or safeguarding devices which initiate a stop signal shall: - Be accompanied with documentation stating the standards that the product meets … - Provide a means for a readily observable indication that the device is operating; - not adversely affected by environmental conditions … - have a maximum response time that shall not be affected by … environmental changes; - provide means for secure attachment; - provide a means to restrict unauthorized adjustments or settings;	fulfilled, see the previous chapters of this report
6.4	Software and firmware-based controllers used in place of hardware based components with safety-related devices shall: a) be designed such that any single safety related component or firmware failure shall: 1) lead to the shutdown of the system in a safe state and 2) prevent subsequent automatic operation until the component failure has been corrected b) supply the same degree of safety achieved by using hardwired/ hardware components per 4.5.4. For example, this degree of safety may be achieved by using microprocessor redundancy, microprocessor diversity, and self-checking c) be certified by a National Recognized Testing Laboratory (NRTL) to an approved standard applicable for safety devices.	fulfilled, see the previous chapters of this report This Test Institute is not listed as a National Recognized Testing Laboratory (NRTL). Despite this matter of fact, the test objects are in accordance with approved standards for safety devices.
10.1	Requirements for safety circuit performance The ultimate design requirement for safety systems is that, should they fail, the associated hazard is left in a safe state…	Fulfilled
11.3	Requirements for safeguarding devices that signal a stop … d) provision of control over adjustments or settings being made by others than authorized personnel e) indication on if the device is functioning	 The RSLogix5000 configuration software provides several access levels. An indication, that the device is functioning, is available.

Result:

The requirements of this standard are met, so far they are applicable. The user still needs to comply with other requirements from the standard including requirements that have an effect on the operation of the safety system.

4.11.7. Requirements according to ANSI B11.19

This standard contains requirements for the design, construction, care and operation of safeguards used at the other ANSI B11 machine tools. The selection and the application of the safeguarding system are provided in the appropriate B11 safety standard for the particular machine tool.

The B11.19 standards provides requirements for different types of safeguards (fixed and movable guards, presence sensing devices, two hand operating control devices, probe protection devices and others).

In the following clauses generally relevant as well as specific requirements are defined.

Clause	Requirements	Result
4.1	Safeguarding supplier	--
4.1.1	The safeguarding supplier Within the scope of its work activity, the safeguarding supplier shall ensure that safeguarding meets the design, construction, integration and installation requirements of this standard.	Fulfilled, as far as applicable for a safety PLC without application
4.1.2	The safeguarding supplier shall furnish documentation as required for the safeguarding, including installation requirements, operating instructions, and maintenance requirements.	All required information is present in the user manual.
6.1	Performance of the safety related function(s). When a component, module, device or system failure occurs, such that it or a subsequent failure of another component, module, device or system would lead to the inability of the safety-related function(s) to respond to a normal stop command or an immediate stop command, the safety-related function shall: • prevent initiation of hazardous machine motion (or situation) until the failure is corrected or until the control system is manually reset; or • initiate an immediate stop command and prevent re-initiation of hazardous machine motion (or situation) until the failure is corrected or until the control system is manually reset; or • prevent re-initiation of hazardous machine motion (or situation) at the next normal stop command until the failure is corrected or until the control system is manually reset.	Fulfilled, as far as applicable for a safety PLC without application

Result:

The requirements of this standard are met, so far they are applicable. The user still needs to comply with other requirements from the standard including requirements that have an effect on the operation of the safety system.

4.11.8. Requirements according to NFPA 79

This standard from the National Fire Protection Association contains the electrical requirements for industrial machinery. In the following clauses generally relevant as well as specific requirements are defined.

Clause	Requirements	Result
4.4	*Physical Environment and Operating Conditions.*	See 4.4.1 and 4.4.2
4.4.1	*General.* The electrical equipment shall be suitable for use in the physical environment and operating conditions specified in 4.4.3 to 4.4.6 and 4.4.8. When the physical environment or the operating conditions are outside those specified, an agreement between the supplier and the user shall be considered.	See 4.4.3 to 4.4.6 and 4.4.8
4.4.2.	*Electromagnetic Compatibility (EMC)*	See 4.4.2.1
4.4.2.1	Transient suppression, isolation, or other appropriate means shall be provided where the equipment generates electrical noise or transients, which can affect the operation of equipment.	Fulfilled, see also chapter 4.9.2
4.4.3*	Ambient Operating Temperature. Electrical equipment shall be capable of operating correctly in the intended ambient air temperature. The ambient operating temperatures for correct operation of the electrical equipment shall be between air temperatures of 5°C and 40°C (41°F to 104°F).	Fulfilled, see also chapter 4.9.1
4.4.4*	*Relative Humidity.* The electrical equipment shall be capable of operating correctly within a relative humidity range of 20 to 95 percent (non condensing). Harmful effects of relative humidity outside the permitted range shall be avoided by design of the equipment or, where necessary, by additional measures (e.g., built-in heaters, air conditioners, humidifiers).	Fulfilled, see also chapter 4.9.1
4.4.5	*Altitude.* Electrical equipment shall be capable of correct operation at altitudes up to 1000 m (3300 ft) above mean sea level. (See Annex B.)	Fulfilled
4.4.6	*Contaminants.* Electrical equipment shall be adequately protected against the ingress of solid bodies and liquids (see Section 11.3). Equipment shall be suitable for the environment where contaminants (e.g., dust, acids, corrosive gases, salt) are present.	The Safety Controller must be mounted within an enclosure that is suitably designed for application specific environmental conditions.

Clause	Requirements	Result
4.4.8	*Vibration, Shock, and Bump.* Undesirable effects of vibration, shock, and bump, including those generated by the machine and its associated equipment and those created by the physical environment, shall be avoided by the selection of suitable equipment, by mounting it away from the machine, or by the use of anti-vibration mountings.	Fulfilled, see also chapter 4.9.1

Clause	Requirements	Result
6.2	Protection Against Direct Contact. Live parts operating at 50 volts rms ac or 60 volts dc or more shall be guarded against contact.	Fulfilled
6.5.3	Discharge of Stored Energy Capacitors shall be provided with a means of discharging stored energy.	Fulfilled
6.5.3.1	Time of Discharge The residual voltage of a capacitor shall be reduced to 50 volts, nominal, or less, within 1 minute after the capacitor is disconnected from the source of supply.	Fulfilled
9.4.3*	*Control Systems Incorporating Software and Firmware Based Controllers.*	See 9.4.3.1 to 9.4.3.4.2
9.4.3.1	*Software Modification.* Programmable electronic systems shall be designed and constructed so that the ability to modify the application program shall be limited to authorized personnel and shall require special equipment or other means to access the program (e.g., access code, key-operated switch).	Fulfilled
9.4.3.2	*Memory Retention and Protection*	See 9.4.3.2.1 to 9.4.3.2.3
9.4.3.2.1	Means shall be provided to prevent memory alteration by unauthorized persons.	Fulfilled
9.4.3.2.2	Loss of memory shall not result in a hazardous condition.	Fulfilled
9.4.3.2.3	Power supplies for electronic equipment requiring memory retention shall have battery backup of sufficient capacity to prevent memory loss for a period of at least 72 hours.	Fulfilled
9.4.3.3	*Software Verification.* Equipment using reprogrammable logic shall have means for verifying that the software is in accordance with the relevant program documentation.	Fulfilled
9.4.3.4	*Use in Safety-Related Functions*	See 9.4.3.4.1 to 9.4.3.4.2
9.4.3.4.1	Software and firmware based controllers to be used in safety-related functions shall be listed for such use.	Fulfilled
9.4.3.4.2	Control systems incorporating software and firm-ware based controllers performing safety-related functions shall conform to all of the following: (1) In the event of any single failure, the failure shall (a) not lead to the loss of the safety function. (b) Lead to the shutdown of the system in a safe state (c) Prevent subsequent operation until the component failure has been corrected (d) Prevent unintended startup of equipment upon correction of the failure (2) Provide protection equivalent to that of control systems incorporating hardwired / hardware components. (3) Be designed in conformance with an approved standard that provides requirements for such systems	 Fulfilled, as far as applicable for a safety PLC without application Fulfilled Fulfilled Fulfilled Fulfilled Fulfilled

Result:

The requirements of this standard are met, so far they are applicable. The user still needs to comply with other requirements from the standard including requirements that have an effect on the operation of the safety system.

4.11.9. Requirements according to NFPA 85

This standard from the National Fire Protection Association contains the Boiler and Combustion Systems Hazards Codes.

In the following tables the relevant general requirements are defined. These requirements are applied to the Safety Controllers and it is described, if they are applicable and how they are fulfilled:

Clause	Requirement	Result
4.11.2	The logic system for burner management shall be designed specifically so that single failure in that system does not prevent an appropriate shutdown.	Needs to be taken into account at application and system level.
4.11.3	The burner management system interlock and alarm functions shall be initiated by one or more of the following: (1) One or more switches or transmitters that are dedicated to the burner management system (2) One or both signals from two transmitters exceeding a preset value (3) The median signal from three transmitters exceeding the preset value	Needs to be taken into account at application and system level.
4.11.3.1	When signals from multiple switches or transmitters are provided to initiate interlock or alarm functions, those signals shall be monitored in comparison to each other by divergence or other fault diagnostic alarms.	Needs to be taken into account at application and system level.
4.11.3.2	When signals from multiple switches or transmitters are provided to initiate interlock or alarm functions, the provided signals shall be generated by individual sensing devices connected to separate process taps.	Needs to be taken into account at application and system level.
4.11.4	Alarms shall be generated to indicate equipment malfunction, hazardous conditions, and misoperation.	Needs to be taken into account at application and system level.
4.11.5	The burner management system designer shall evaluate the failure modes of components, and as a minimum the following failures Failure Effects (logic system). (1) Interruptions, excursions, dips, recoveries, transients and partial losses of power (2) Memory corruption and losses (3) Information transfer corruption and losses (4) Inputs and Outputs (fail-on, fail-off) (5) Signals that are unreadable or not being read (6) Failure to address errors (7) Processor faults (8) Relay coil failure (9) Relay contact failure (fail-on, fail-off) Timer failure	See documentation in the other chapters of this document.

Clause	Requirement	Result
4.11.6	The design of the logic system for burner management shall include and accommodate the following requirements: (1) Diagnostic shall be included in the design to monitor processor logic function (2) Logic system failure shall not preclude proper operator intervention (3) Logic shall be protected from unauthorized changes (4) Logic shall not be changed while the associated equipment is in operation (5) System response time (through-put) shall be short to prevent negative effects on the application (6) Protection from the effects of noise shall prevent false operation (7) No single component failure within the logic system shall prevent a mandatory master fuel trip (8) The operation shall be provided with a dedicated manual switch(es) that shall actuate the master fuel trip relay independent and directly (9) At least one manual switch ref in 4.11.6(8) shall be identified and located remotely where it can be reached in case of emergency (10) The logic system shall be monitored for failure (11) Failure of the logic system shall require a fuel trip for all equipment supervised by the failed logic system (12) Logic shall be maintained either in nonvolatile storage or in other memory that retains information on the loss of system power.	(1) through (7) are fulfilled: See documentation in the other chapters of this document. (8) Has to be considered at the system level. (9) Has to be considered at the system level. (11) Has to be considered at the system level. (12) Has to be considered at the system level.
4.11.7.1	Except as noted in 4.11.7.2, the burner management system shall be provided with independent logic, independent logic solving hardware, independent input/output systems, and independent power supplies and shall be a functionally and physically separate device from other logic systems.	Has to be considered at the overall system level.
4.11.7.2	For single burner boilers, boiler control systems shall be permitted to be combined with the burner management system under one of the following conditions: 1. If the fuel/air ratio is controlled externally from the boiler control system 2. If the combined boiler control system and burner management system is specifically listed or labeled for the application	Has to be considered at the overall system level.
4.11.7.3	The burner management safety functions shall include, but shall not be limited to, purge interlocks and timing, mandatory safety shutdowns, trial timing for ignition, and flame monitoring.	Needs to be taken into account at application level.
4.11.7.4	The logic system shall be limited to one boiler or HRSG.	Has to be considered at the overall system level.

Clause	Requirement	Result
4.11.7.6	Network communication between burner management system and other systems shall be permitted. The network communication with other systems shall not be the same network that the burner management system uses to communicate with its input / output hardware.	Has to be considered at the overall system level.
4.11.7.7	Signals and the manually operated devises specified in 4.11.6(8) that initiate mandatory master fuel trips shall be hardwired.	Has to be considered at the overall system level.
4.11.8.1	Logic sequences or devices intended to cause a safety shutdown, once initiated, shall cause a burner or master fuel trip, as applicable, and shall require operator action prior to resuming operation of the affected burner(s).	Logic sequences needs to be implemented by the end user at the application level.
4.11.8.2	No logic sequence or device shall be permitted that allows momentary closing and subsequent inadvertent reopening of the main or ignition fuel valves.	Logic sequences needs to be implemented by the end user at the application level.
4.11.9	Circuit Devices. No momentary contact or automatic resetting device, control, or switch that can cause chattering or cycling of the safety shutoff valves shall be installed in the wiring between the load side (terminal) of the primary or programming control and the main or ignition fuel valves.	Logic sequences needs to be implemented by the end user at the application level.
4.11.10	Documentation. Documentation shall be provided to the owner and operator, indicating that all safety devices and logic meet the requirements of the application.	User Documents / Safety Manual

Result:

No contradictions were identified by the assessment in reference with the requirements of the [S6] chapter 4.11 “Burner Management System Logic”.

The user is responsible for the compliance with all other requirements from the standard including requirements that have an effect on the operation of the safety system. The end-user should refer to the User Documents and Safety Manual

Logic sequences initiating the safety shutdown shall be implemented as application and were not subject of this assessment.

4.11.10. Requirements according to NFPA 86

This standard from the National Fire Protection Association outlines the requirements for ovens and furnaces.

In the following tables the relevant general requirements are defined. These requirements are applied to the Safety Controllers and it is described, if they are applicable and how they are fulfilled:

Clause	Requirement	Result
8.4.2.1	(E) The PLC shall detect the following conditions: (1) Failure to execute any program or task containing safety logic (2) Failure to communicate with any safety input or output (3) Changes in software set point of safety functions (4) Failure of outputs related to safety functions (5) Failure of timing related to safety functions	See documentation in the other chapters of this document.
	(F) A safety shutdown shall occur within 3 seconds of detecting any condition listed failures in (E)	The safety shutdown occurs within 135ms: See [D1] chapter 5.35

Clause	Requirement	Result
8.4.2.2	Hardware (A) Memory that retains information on loss of system power shall be provided for software	(A) application software, firmware stored in FLASH - memory
	(B) The PLC shall have a minimum mean-time-between failures (MTBF) rating of 250,000 hours	(B) $MTTF_D \geq 100y=876.000$ hours
	(D) Output checking shall be provided for PLC outputs controlling fuel safety shutoff valves and oxygen safety shutoff valves.	See documentation in the other chapters of this document.
8.4.2.3	Software (A) Access to the PLC and its logic shall be restricted to authorized personnel.	Password for safety application can be applied by the configuration tool RSLogix 5000
	(B) The following power supplies shall be monitored: i. Power supplies used to power PLC inputs and outputs that control furnace safety functions	Fulfilled, see documentation in the other chapters of this document.
	(C) When any power supply required by 8.4.2.3 (B) (1) fails, the dedicated PLC output required in 8.4.2.1(G) shall be deactivated.	Has to be considered during the application design. Possibility is given by the PLC. See documentation in the other chapters of this document.
	(E) Software shall be documented as follows i. Labeled to identify elements or group of elements containing safety software ii. Labeled to describe the function of each element containing safety software.	See documentation in the other chapters of this document.
8.4.5	Safety PLC (A) Where used for combustion safety service, safety programmable logic controllers shall have the following characteristics: (1) The processor and the input and output (I/O) shall be listed for control reliable service with an SIL rating of at least 2. (2) Access to PLCs dedicated to safety functions shall be restricted. (3) Non-safety functions, where implemented, shall be independently accessible from safety functions. (4) All safety function sensors and final elements shall be independent of operating sensors and final elements.	See documentation in the other chapters of this document.

Result:

No contradictions were identified by the assessment in reference with the requirements of the [S7].

The user is responsible for the compliance with all other requirements from the standard including requirements that have an effect on the operation of the safety system. The end-user should refer to the User Documents and Safety Manual.

Logic sequences performing application depending safety functions (e.g. timed pre-ignition purge) were not subject of this assessment.

4.12. Programming and configuration

The programming and configuration tool RSLogix 5000 has not been inspected during this current type approval of the Safety Controller. For the corresponding inspection results please refer to the former test report [R7]. The standards [S2] and [S3] have already be part of former assessments. The customer is an ISO 9001 certified company (see document **Fehler! Verweisquelle konnte nicht gefunden werden.**) also for design.

Result:

Due to the fact that the programming and configuration tools have not been changed and the standards [S2] and [S3] have already been considered in former assessments and the customer is ISO 9001 certified, it is concluded that also the requirements of [S1] part 3 regarding off-line tools (section 7.4.4) are fulfilled.

4.13. Communication requirements

The Safety Controller uses the already developed and certified [R7] CIP-safety protocol, to communicate to safety devices. The safety protocol has not been changed. For the respective corresponding test results determined in the past, please refer to the respective test report [R7].

The integration of the safety protocol into the Safety Controller has been tested during the current type approval. The tests are specified in the Safety Protocol Conformance Test Strategy **Fehler! Verweisquelle konnte nicht gefunden werden.** and the test results are reported in the Safety Protocol Test Summary.
Fehler! Verweisquelle konnte nicht gefunden werden.
Result:

The Test Institute accepts the test results and the requirements for a software integration of a safety protocol are met.

5. Summary

The GuardLogix- SIL3-Controller 1756-L7xS and 1756-L7SP complies with the requirements of the relevant standards:

EN ISO 13849-1	Cat. 4 / PL e
EN 62061	SIL CL 3
IEC 61508	SIL 3

Hence it is suitable for the use in applications up to Cat. 4 / PL e acc. to EN ISO 13849-1 and SIL 3 acc. to EN 62061 / IEC 61508.

The instructions of the safety reference manual and user manual shall be considered ([U1 -U4]).

Even if the configuration software and the safety design of the modules perform every possible check, the user is obliged to verify the correct execution of every safety function within an application before commissioning of a machine.

The current versions of components are also shown in the Revision Release List ([T6]).

Cologne, 2012-02-08
TIS/A-FS/Kst. 968 hei-nie

Report released after review:
Date: 2012-02-08

The inspectors

Dipl.-Ing. Robert Heinen | Dipl.-Ing. Gernot Klaes | Dipl.-Ing. (FH) Oliver Busa